Führendes Luft- und Raumfahrtunternehmen macht Ransomware-Betrügern den Garaus

Wie HarcoSemco einen CryptoLocker-Angriff dank Barracuda Backup per Knopfdruck abgewehrt hat.

Der Angriff

Seit die bekannte CryptoLocker-Ransomware zusammen mit zahlreichen Varianten im Jahre 2013 zum ersten Mal auftrat, wurde sie eingesetzt, um Unternehmen auf der ganzen Welt um Milliarden von Dollar zu erpressen. Als damit allerdings HarcoSemco, ein führender Hersteller von Luft- und Raumfahrtkomponenten, angegriffen wurde, war IT-Manager Brian O'Connor entschlossen, die verschlüsselten Daten zurückzubekommen und die Betrüger mit leeren Händen zurückzulassen.

„Es war schrecklich", so O'Connor über den Morgen, an dem Mitarbeiter bei ihrer Ankunft feststellen mussten, dass ihre Dateien unzugänglich waren und auf ihrem Bildschirm ein beängstigendes Bild zu sehen war. „Alle waren völlig durcheinander, aber wir wollten das Lösegeld nicht bezahlen."

Laut O'Connor wurden bei dem Angriff öffentliche Ordner und sogar ein Server mit Live-Finanzdaten infiziert, was für das Unternehmen eine enorme Gefahr dargestellt hätte. Allein die potenzielle Rufschädigung für HarcoSemco wäre untragbar gewesen.

> „Barracuda Backup hat genau so funktioniert, wie es sollte. Es ging leicht, es ging schnell und unsere Angreifer haben nichts bekommen."
>
> **Brian O'Connor**
> IT-Manager
> HarcoSemco

Profil

- Zentrale: Branford im US-Bundesstaat Connecticut
- Ein anerkannter Hersteller von Luft- und Raumfahrtkomponenten
- Über 60 Jahre Branchenerfahrung

Herausforderungen

- Wiederherstellung kritischer Daten, die von CryptoLocker gesperrt wurden
- Hohe Lösegeldforderung der Angreifer
- Minimierung der Ausfallzeiten bei der Wiederherstellung

Lösung

Barracuda Backup

Ergebnisse

- Keine Lösegeldzahlung
- Keine signifikanten Ausfallzeiten
- Sorgenfreiheit

Die Reaktion

Als O'Connor zu HarcoSemco kam, verwendete das Unternehmen zur Datensicherung ein bandbasiertes System. Die Einschränkungen, die solche Systeme mit sich bringen (sie sind zeit- und arbeitsintensiv, lassen sich schlecht skalieren, Sicherungsdateien werden nicht oft genug aktualisiert, und sie können unzuverlässig sein), ließen ihn bald nach einer neuen Lösung suchen.

„Unsere Schwesterfirma in Kalifornien verwendete Carbonite EVault. Also haben wir uns das angesehen“, so O'Connor. „Wir fanden die Lösung aber ein wenig umständlich. Daraufhin wandte ich mich an TBNG Consulting und man machte uns auf das Produkt von Barracuda aufmerksam. Nach einer erfolgreichen Testphase bestellte O'Connor zwei Barracuda Backup 690-Geräte. Eines wurde in der Niederlassung in Branford installiert und mit dem anderen wurde die Carbonite-Lösung des kalifornischen Unternehmens ersetzt. Jedes Gerät replizierte die lokal gesicherten Dateien auf das jeweils andere. Sieben Jahre später wird die gleiche Lösung immer noch produziert, auch wenn HarcoSemco auf 790er Modelle mit höherer Kapazität aufgerüstet hat.

Als CryptoLocker also die Kontrolle über die Unternehmensdateien übernahm und einige Mitarbeiter in Panik gerieten, machte sich O'Connor einfach an die Arbeit. Er löschte die infizierten Dateien und stellte sie aus den letzten Sicherungsdateien wieder her. „Zuerst habe ich Daten schrittweise wiederhergestellt, bevor ich das ganze Ausmaß der Angriffe erkannte“, erinnert sich O'Connor. „Letztendlich habe ich mich dann dazu entschlossen, den gesamten Server wiederherzustellen. Barracuda Backup hat genau so funktioniert, wie es sollte. Es ging leicht, es ging schnell und unsere Angreifer haben nichts bekommen.“

Ausblick

„Ich bin immer überrascht, wenn ich höre, dass ein Unternehmen Lösegeld zahlen musste oder wegen Ransomware kritische Daten verloren hat“, so O'Connor. „Mit jeder anständigen, modernen Backup-Lösung, die gut verwaltet wird, sollte sich das verhindern lassen. Dennoch hebt sich Barracuda Backup aufgrund seiner Benutzerfreundlichkeit, der flexiblen Replikationsoptionen und der Skalierbarkeit von Vergleichsprodukten ab.“

Bei HarcoSemco freut man sich auf einige Änderungen, welche die von O'Connor erwähnte Flexibilität besonders nützlich machen könnten. „Unsere kalifornische Schwesterfirma schließt bald“, so O‘Connor. „Deshalb werden alle Daten von dort hierher verlagert und wir müssen unsere Replikationsstrategie überdenken. Außerdem wird eine neue Niederlassung in Mexiko eröffnet und dies müssen wir ebenso im System berücksichtigen.

Eine Herausforderung stellt für O'Connor die Einhaltung der ITAR, der Verordnung über den internationalen Waffenhandel, dar. „Als wir die Barracuda Backup-Appliances erhielten, waren wir der Meinung, dass die Verwendung der Cloud-Replikationsfunktion des Produkts ein gewisses Risiko für die ITAR-Compliance darstellen könnte“, so O‘Connor. „Dieses Thema werden wir wahrscheinlich noch einmal unter die Lupe nehmen, sobald die Umgestaltung des Unternehmens in Gang gekommen ist. Sollte sich die Cloud-Replikation unserer Datensicherungen als ITAR-konform erweisen, könnte sie im Hinblick auf die Skalierbarkeit und die langfristige Geschäftskontinuität sehr hilfreich sein.“

Weitere Informationen zu Barracuda Backup

https://de.barracuda.com/products/backup

Barracuda
Your journey, secured.